The Heritage Foundation

ISSUE BRIEF

No. 4557 | MAY 4, 2016

Understanding the Internet of Things

Riley Walters

The term "Internet of Things" (IoT) refers to all electronic devices that are connected and communicate information across a network or networks. Consumers may have experience with IoT technology from the use of wearable devices such as smart watches or fitness trackers. For manufacturers, it is often associated with increased automation (Industry 4.0). The IoT also infers the interconnection of homes, transportation systems, utility systems, and even entire cities ("smart cities") in what some have termed the "Internet of Everything."

With newer technologies and greater interconnectivity, the IoT environment will continue to expand and potentially create more connected and efficient regional and global economies. Greater reliance on interconnected devices and the combination of cyber and physical devices will generate new security vulnerabilities. While it is important to ensure user security, Congress and regulators should refrain from using regulations to preempt unknown risks that might deter the innovation and development of newer technologies.

Defining the Internet of Things

Greater reliance on the collecting and sharing of digital information across devices and various industries and sectors has a great many implications for matters of policy. IoT policy involves many different issues including privacy, security, supply chains, data collection and storage, spectrum, cybersecurity, consumer goods, critical infrastructure, and a number of economic concerns.

The IoT is already expansive and will continue to grow exponentially. Industry estimates of the number of IoT devices by 2020 range from 39 billion to 200 billion, compared to the estimated 13 billion devices today.1 This includes wearable devices like fitness trackers, home devices such as thermostats or coffee makers, farming devices like watering systems, autonomous vehicles, robotics, transportations systems, and telecommunications. Given the multitude of effects that the IoT has on daily life, as well as the impact that so many other policy areas might have on the IoT environment, Congress should be mindful of how profoundly legislation could affect the future of the IoT.

One way the government in particular will affect the IoT's future is through numerous agencies that have or want to have authority to regulate areas of the IoT.

- The Federal Trade Commission (FTC) will seek to promote consumer security.
- The Federal Communications Commission (FCC) will pursue issues of spectrum and how this affects IoT devices.
- The Department of Commerce (DOC) will review the economic implications of increased data and automation.

This paper, in its entirety, can be found at
http://report.heritage.org/ib4557

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

- The Department of Homeland Security (DHS) will explore both cyber and physical threats to critical infrastructure.

- Agencies within the Department of Agriculture (DOA), Department of Energy (DOE), Department of Transportation (DOT), and Department of Health and Human Services (HHS) will each have some role in regard to a growing IoT.

A Working Group on the Internet of Things

Given the growing IoT environment and interest from regulators, Congress has begun to consider the IoT. The Developing Innovation and Growing the Internet of Things (DIGIT) Act seeks to create a commission crafted of representatives from the DOT, FCC, FTC, National Science Foundation, DOC, and Office of Science and Technology Policy to examine IoT proliferation.

The commission would consult with non-government stakeholders from businesses, manufacturers, consumer groups, and other entities with relevant expertise, as determined by the Secretary of Commerce. This includes examining spectrum needs, regulatory environment, consumer protection, privacy, security, and federal preparedness as DHS and the Office of Management and Budget become involved. The commission would seek to make recommendations on how Congress can plan for and encourage IoT proliferation in the U.S.

The private sector will be the most affected by any regulations made by Congress or regulatory agencies. It is therefore important that companies play more than simply a consulting role.

The proliferation and efficacy of the IoT come from the immediate sharing of information between devices, certain functions working autonomously, and consumers benefiting from this increase of functionality. Congress should be aware that the legislative and regulatory processes move at a pace much slower than new technology comes to fruition. New policies, especially those made ad hoc, not only will end up applying out-of-date rules, but also may create duplicative regulation from a number of agencies such as the DOT, DHS, and FCC. As a result, IoT producers and consumers may be forced to contend with conflicting regulations.

Formal legislation calling for the creation of a committee simply highlighting IoT use would seem to be unnecessary as so many government stakeholders have or will have more of a vested interest in the IoT. A limited benefit of a government-led IoT working group would be to help determine jurisdictional challenges to avoid repetitive or conflicting regulations.

A commission would also be challenged by the size and scope of the IoT issue. Contested and complex topics such as privacy, encryption, and spectrum will likely be addressed by this commission, but a single commission that attempted to address so many contentious issues might well end up making superficial recommendations. For example, attempting to assess the IoT and spectrum use of the IoT in a single working group would likely diminish or short-change other uses of spectrum outside of the IoT.

Next Steps for the Internet of Things

As the Internet of Things proliferates, Congress, the Administration, and regulators should:

- **Avoid seeking a formal commission at this time.** It is important that Congress both understand the growing IoT environment and support the IoT and new technologies. There are, however, still questions about how a formal commission would attempt to examine the IoT, security, privacy, spectrum, and other issues efficiently enough to craft meaningful recommendations for Congress.

- **Refrain from stove-piping larger policies within the context of the IoT.** Broader issues such as privacy, security, spectrum, or the economy will each affect IoT proliferation in its own way. These broad issues should not be refrained divided and marginalized simply to be addressed within the context of the IoT. While it is important to understand the greater impact of the growing

[1] Intel, "A Guide to the Internet of Things Infographic," http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html (accessed April 22, 2016), and news release, "'Internet of Things' Connected Devices to Almost Triple to Over 38 Billion Units by 2020," Juniper Research, July 28, 2015, http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020 (accessed April 22, 2016).

IoT environment, policies should continue to be addressed individually. The IoT should be considered more within the context of these issues.

- **Allow the IoT to flourish.** It is easier to see current trends in technology than to know where technology and the IoT will be 10 years from now. Congress and regulators should avoid attempts to craft laws to deal with challenges that IoT proliferation *might* bring. It is important to let the IoT develop within the private sector; only when a genuine risk seems to be developing should policymakers evaluate the impact of new regulation.

Advancing a Secure, Free Internet of Things

There are still varying definitions of the IoT, ranging from as simple as interconnecting devices or objects to the more complex interconnection of industries, transportations systems, and cities. How stakeholders come to define the IoT and understand how varying domestic and international stakeholders define the IoT will have implications on future policy.

There exist concerns about the impact that the growing IoT will have on issues of security, the economy, and society as a whole. It is important to address each issue separately as it becomes a cause for concern. Attempting to address all issues simultaneously under the IoT umbrella could cause the government to neglect important issues while focusing on topics that are best handled by the private sector.

*—**Riley Walters** is a Research Assistant in the Douglas and Sarah Allison Center for Foreign Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*